On Lower Bounds Of Character Sums

A THESIS
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCES
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE

BY
FERRUH ÖZBUDAK
JUNE, 1995

ON LOWER BOUNDS OF CHARACTER SUMS

A THESIS

SUBMITTED TO THE DEPARTMENT OF MATHEMATICS

AND THE INSTITUTE OF ENGINEERING AND SCIENCES

OF BILKENT UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE

By

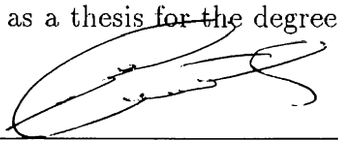
Ferruh Özbudak

June, 1995

Ferruh ÖZBUDAK

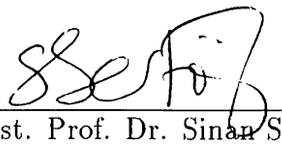
tarafından bağışlanmıştır

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.



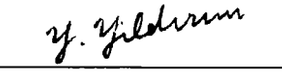
Prof. Dr. S.A. Stepanov(Principal Advisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.



Asst. Prof. Dr. Sinan Sertöz

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.



Asst. Prof. Dr. Yalçın Yıldırım

Approved for the Institute of Engineering and Sciences:

Prof. Dr. Mehmet Baray
Director of Institute of Engineering and Sciences

ABSTRACT

ON LOWER BOUNDS OF CHARACTER SUMS

Ferruh Özbudak
M.S. in Mathematics
Advisor: Prof. Dr. S.A. Stepanov
June, 1995

In this work we extended the results of S.A. Stepanov [3], [1] about lower bounds for incomplete character sums over a prime finite field F_p to the case of arbitrary finite field F_q. Moreover we also applied Goppa's construction to superelliptic curves with a lot of rational points to construct rather good geometric Goppa codes.

Keywords : Finite field, character sum, linear code, Goppa code.

ÖZET

KARAKTER TOPLAMLARININ ALT SINIRLARI ÜZERİNE

Ferruh Özbudak
Matematik Bölümü Yüksek Lisans
Danışman: Prof. Dr. S.A. Stepanov
Haziran, 1995

Bu çalışmada S.A. Stepanov'un [3], [4] bir asal sonlu cisim F_p'nin eksik olabilen karakter toplamlarının alt sınırları hakkında yaptığı çalışmalar herhangi bir sonlu cisim F_q için genelleştirildi. Ayrıca Goppa'nın kod bulma metodu da üzerinde çok fazla rasyonel nokta bulunan süpereliptik eğrilere uygulandı.

Anahtar Kelimeler : Sonlu cisim, karakter toplamı, doğrusal kod, Goppa kodu.

ACKNOWLEDGMENTS

I am grateful to Prof. Dr. S.A. Stepanov who introduced me the marvellous world of finite fields, algebraic curves and coding theory, and expertly guided my research by his wonderful ideas in all steps.

I would like to thank to Asst. Prof. Dr. Sinan Sertöz for his encouragement and for his readiness to help at all times.

I would like to thank to my family for their unfailing support and influence in my life.

Finally, I would like to thank to all my friends, especially Feza and Kırdar, for sharing their brilliance and a lot more with me.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

Finite fields are interesting basically due to the fact that Galois Theory is complete via Frobenius automorphism. We will give two applications of finite fields in this thesis.

In the first half we deal with lower bounds of incomplete character sums over finite fields. In Chapter 2 basic structure of finite fields, multiplicative and additive characters are given. We generalize the wonderful method of Stepanov about lower bounds of incomplete quadratic character sums of polynomials over prime finite fields, in Chapter 3.

The second part begins with Chapter 4, which gives basic definitions of linear codes. We apply superelliptic curves with a lot of rational points to Goppa construction in Chapter 5. We conclude with Chapter 6.

Chapter 2

PRELIMINARIES 1

This chapter contains a very limited exposition of finite fields, multiplicative and additive characters of finite fields. Most of the proofs are referred to Stepanov [1] or Schmidt [7]. The reason is the fact that the proofs are easy to understand and they are very well explained in above books and Lidl [8]. The chapter ends with the statement of the A. Weil's result on bounds of character sums of polynomials.

2.1 Finite Fields

A finite field with q elements is denoted by F_q. Since F_q is a field, q may not be any positive integer but either a prime p or a positive integer power of a prime p^m. The typical examples are F_2 and F_4.

1. $q = 2$, $F_2 = \{0, 1\}$.
2. $q = 2^2$, $F_4 = \{0, 1, \alpha, 1 + \alpha\}$, where $\alpha^2 + \alpha + 1 = 0$.

Formally we have the following theorem.

Theorem 1 *If F_q is a finite field of order q, then $q = p^k$, p a prime. For every such q, there exists exactly one field F_q. This field is the splitting field of $x^q - x$ over F_p, and all of its elements are roots of $x^q - x$.*

PROOF. See for example Schmidt [7], Theorem 1.1A. ∎

Corollary 1 *$F_{q_1} \subset F_{q_2}$ iff $q_1 = p^{k_1}$, $q_2 = p^{k_2}$, and $k_1 \mid k_2$.*

Therefore for any characteristic $p > 0$, we have a tree structure of finite fields of characteristic p where F_p is the base of the tree.

Moreover the algebraic closure is simply the union of all elements of this tree, namely

$$\bar{F}_p = \cup_{s=1}^{\infty} F_{p^s}.$$

Theorem 2 *$F_q^* = F_q \setminus \{0\}$ is a multiplicative group of order $q-1$ which is cyclic.*

PROOF. If $q = p$, then this fact follows from Gauss's theorem (see for example Niven [16], Theorem 2.36). If $q = p^n$, then F_q is a separable extension, and this follows by primitive elements theorem, which generalizes the theorem of Gauss. ∎

eg. $F_4^* = \{\alpha, \alpha^2, \alpha^3\} = \{1, \alpha, 1+\alpha\}$

2.2 Multiplicative Characters of F_q^*

A group homomorphism χ from a multiplicative group F_q^* to the multiplicative group $\mathbb{C}^*$ is called a *multiplicative character* of F_q^*. Thus

$$\chi : F_q^* \to \mathbb{C}^*, \text{ so that}$$
$$\chi(ab) = \chi(a)\chi(b) \text{ for all } a, b \in F_q^*.$$

Note that $\chi(1) = 1$ and $\mid \chi(a) \mid = 1$ for any $a \in F_q^*$.

If χ_1 and χ_2 are multiplicative characters of F_q^*, then there exists a multiplicative character of F_q^* denoted by $\chi_1\chi_2$ and defined by

$$\chi_1\chi_2(a) = \chi_1(a)\chi_2(a) \text{ for every } a \in F_q^*.$$

Moreover χ_1^{-1} which is defined as

$$\chi_1^{-1}(a) = \overline{\chi_1(a)}$$

is also a multiplicative character of F_q^*. Therefore the set of multiplicative characters of F_q^* forms a group, denoted by $\hat{F}_q^*$, called as the *dual group* of F_q^*.

$\hat{F_q^*}$ is also a cyclic group of order $q-1$. If g is a generator of F_q^*, then there exists a generator χ of $\hat{F_q^*}$ defined by

$$\chi(g^t) = e^{\frac{2\pi it}{q-1}} \text{ for every } t \in \mathbb{Z}, \ (t, q-1) = 1 \text{ or } t = 0.$$

The unity of $\hat{F_q^*}$ is called as the *principal character* and denoted by χ_0.

We say χ is *of order* d if $\chi^d = \chi_0$ and d is the smallest such positive integer.

We say χ is *of exponent* s if $\chi^s = \chi_0$, i.e. $d \mid s$.

We can extend the domain of definition of any multiplicative character χ to F_q via

$$\chi(0) = \begin{cases} 1 & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases}$$

There exists orthogonality relations among the characters as stated in the following theorem:

Theorem 3

i) 1) $\displaystyle\sum_{x \in F_q^*} \chi(x) = \begin{cases} q-1 & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$

2) $\displaystyle\sum_{\chi \in \hat{F_q^*}} \chi(x) = \begin{cases} q-1 & \text{if } x = 1, \\ 0 & \text{otherwise,} \end{cases}$

ii) Let $s \mid q-1$

$$\sum_{x \text{ of exponent } s} \chi(x) = \begin{cases} s & \text{if } x \in (F_q^*)^s, \\ 0 & \text{if } x \notin (F_q^*)^s, \ x \neq 0, \\ 1 & \text{if } x = 0. \end{cases}$$

PROOF. See for example Schmidt [7], Theorem 2.1D, Lemma 2.1A. ∎

Note that duality is transparent in i), and ii) is an extension of i).

Moreover the orthogonality relations hold for the complete linear character sums of F_q^* or $\hat{F_q^*}$. It is very difficult to find bounds for arbitrary incomplete sums. In chapter 2, however we generalize Stepanov's method which deals with not only for comlete sums but also for incomplete sums as well.

2.3 Additive Characters of F_q

An *additive character* ψ of F_q is a homomorphism from its additive group to the multiplicative group $\mathbb{C}^*$. Thus

$$\psi : F_q \to \mathbb{C}^*, \text{ so that}$$
$$\psi(a+b) = \psi(a)\psi(b) \text{ for all } a, b \in F_q^*.$$

Note that $\psi(0) = 1$.

There exists a natural map from F_q, $q = p^m$ to F_p, called as the *trace* of F_q over F_p which is defined by

$$tr(x) = x + x^p + \cdots + x^{p^{m-1}} = x + \phi(x) + \cdots + \phi^{m-1}(x),$$

where

$$\phi : x \mapsto x^p$$

is the Frobenius automorphism of F_q fixing F_p.

Theorem 4 *Every additive character of F_q is of the type*

$$\psi_a(x) = e^{\frac{2\pi i tr(ax)}{p}}, \text{ for all } x \in F_q,$$

for some a.

PROOF. See for example Schmidt [7] Lemma 2.2D. ∎

2.4 A. Weil's Result on Character Sums (1949)

Theorem 5 *If*

1) *m is the number of distinct roots of $f(x) \in F_q[x]$ in its splitting field over F_q,*

2) *χ is a nontrivial multiplicative character of order s,*

3) *$f(x)$ is not an s-th power of any polynomial,*

then

$$|\sum_{x\in F_q}\chi(f(x))|\leq (n-1)q^{1/2}.$$

Original proof of this result was based on the use of very powerful methods of abstract algebraic geometry over algebraically non-closed fields. An elementary proof of the theorem was given for the first time by Stepanov. See, Stepanov [1], Theorem 1, page 56.

Chapter 3

ON LOWER BOUNDS OF INCOMPLETE CHARACTER SUMS

3.1 Introduction

Let $p > 2$ be a prime number, F_p be a prime finite field with p elements which we identify with the set $\{1, 2, \ldots, p\}$. Let $f(x)$ be a polynomial of degree > 1 with coefficients in F_p and define

$$S_p(f) = \sum_{x \in F_p} (\frac{f(x)}{p})$$

where $(\frac{a}{p})$ is the Legendre symbol :

$$(\frac{a}{p}) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0 \text{ and } a \text{ is a square in } F_p \\ -1 & \text{if } a \text{ is not a square in } F_p \end{cases}$$

A.A. Karatsuba [12] and D.A. Mit'kin [15] proved the existence of a square-free polynomial in $F_p[x]$ of degree $n \geq 2(\frac{p \log 2}{\log p} + 1)$ for which

$$S_p(f) = \sum_{x=1}^{p} (\frac{f(x)}{p}) = p$$

Therefore the Weil estimate (see Section 2.4) cannot be sharpened essentially,

for example to

$$|\sum_{x\in F_q}\chi(f(x))| \leq ((m-1)q)^{1/2}$$

Later S.A. Stepanov [4] gave a very simple proof of this result by using Dirichlet pigeon-hole principle and extended it to the case of incomplete sums

$$S_N = \sum_{x=1}^{N}(\frac{f(x)}{p}),\ 1 \leq N \leq p$$

Namely, he proved the existence of a square-free polynomial $f(x) \in F_p[x]$ of degree $\geq 2(\frac{(N+1)\log 2}{\log p}+1)$ for which

$$S_N(f) = \sum_{x=1}^{N}(\frac{f(x)}{p}) = N.$$

In his book [1] (section 2.1.3 problem 15) S.A. Stepanov has shown that the same method can be used to get similar results for an additive character.

We will prove the following theorem which gives an extension of this result to the case of an arbitrary nontrivial multiplicative characters of arbitrary finite field F_q.

Theorem 6 *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ an arbitrary subset of F_q, and χ a nontrivial multiplicative character of F_q. Let $s > 1$ be an exponent of χ. Assume $N = c(q)\log q$ and $n \geq 1$ is an integer satisfying*

$$n \geq \frac{N\log s}{\log q} - \frac{N\log(1-\frac{1}{q}) + \log(1 - K_q(1-\frac{1}{q})^{-N})}{\log q} + \frac{\log(1-s^{-N})}{\log q} + R_{N,q} \quad (2.1)$$

where

$$0 \leq K_q \leq 5\log\frac{q}{q-1} \quad (2.2)$$

and

$$|R_{N,q}| \leq (M\frac{\log q}{q})^2\ \frac{1}{(1-\frac{1}{q})^N - K_q} \quad (2.3)$$

and also where:

(i) if $c(q) \to \infty$ as $q \to \infty$, then $M = \frac{e}{\log s}$

(ii) if there exists C' such that $c(q) \leq C'$ as $q \to \infty$, then $M = C'$

Then there exist at least $s-1$ distinct monic s power free polynomials $h_i(x)$, $i=1,2,\ldots,s-1$ in $F_q[x]$ of degree $\leq sn$ such that

$$\sum_{j=1}^{N} \chi(h_i(x_j)) = N$$

for each $i=1,2,\ldots,s-1$.

Remark 1 *Theorem 6 can be compared with the Elliot's result on a lower bound of least nonresidue for a prime finite field.*
Let χ be a nontrivial multiplicative character of F_q of exponent s. Let $s < q^{1/2}$. Define $A_{q,s} = \{f \in F_q[x] : f \notin (F_q[x])^s \text{ and } deg f \leq s\}$. There exists a subset $B \subseteq F_q^*$ such that $f(B) \not\subseteq (F_q)^s$ for each $f \in A_{q,s}$, for instance $B = F_q^*$ by Weil's result.
Define $h(q,s)$ as the minimum of the cardinalities of the sets satisfying the property that $B \subseteq F_q^*$ and $f(B) \not\subseteq (F_q)^s$ for each $f \in A_{q,s}$. Then as a result of Theorem 6 $h(q,s) > d_s \log q$ for large q where $d_s > 0$.
Define $B_{g(p,s)} = \{1,2,\ldots,g(p,s)\} \subseteq F_p^*$. If $f(B_{g(p,s)}) \not\subseteq (F_p)^s$ for each $f \in A_{p,s}$, then $g(p,s) \geq h(p,s) > d_s \log p$ for large p where $d_s > 0$.
This result is similar to Elliot's result [14], [13] :
If $f(B_{g(p,s)}) \not\subseteq (F_p)^s$ for $f(x) = x$, then $g(p,s) > d_s \log p$ for infinitely many p where $d_s > 0$.
Note that our result holds for each sufficiently large prime number while Elliot's result holds only for infinitely many prime numbers.

For the incomplete additive character sums we will prove the following theorems. Denote by ψ a nontrivial arbitrary additive character of F_q, i.e.

$$\psi(x) = e^{2\pi i \frac{tr(\alpha x)}{p}} \text{ , where } \alpha \in F_q^*$$

For simplicity we can restrict ourselves to the case $\alpha = 1$.

Theorem 7 *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ an arbitrary subset of F_q, and $0 < \epsilon < \frac{1}{2\pi}$. Let $1 \leq n \leq q^{1/2}$ be an integer satisfying*

$$n - [\frac{n}{p}] \geq \frac{N \log[\frac{p-1}{p\epsilon} + 1]}{m \log p} + \frac{\log(2 + [\frac{p-1}{p\epsilon} + 1]^{-N})}{m \log p} \tag{2.4}$$

Then there exists a polynomial $f(x) \in F_q[x]$ such that $1 \leq deg f \leq n$,

$$tr(f(F_q)) \neq \{0\} \text{ , i.e. not identically zero on } F_q \tag{2.5}$$

and

$$|\sum_{j=1}^{N}\psi(f(x_j))| \geq N(1-2\pi\epsilon) \tag{2.6}$$

For large p we can improve Theorem 7 by a stronger condition on f.

Theorem 7' *Let $q=p^m$, p a prime number, $B=\{x_1,x_2,\ldots,x_N\}\subseteq F_q$ an arbitrary subset of F_q, and $0<\epsilon<\frac{1}{2\pi}-\frac{1}{p}$. Let $n\geq 1$ be an integer satisfying*

$$[\frac{n+1}{m}] \geq \frac{N\log[\frac{p+p\epsilon}{1+p\epsilon}]}{\log p}+\frac{\log(1+[\frac{p+p\epsilon}{1+p\epsilon}]^{-N})}{\log p} \tag{2.7}$$

Then there exists a polynomial $f(x)\in F_q[x]$ of degree $\leq n$ such that

$$tr(f(B))\neq\{0\}\ ,\ i.e.\ not\ identically\ zero\ on\ B$$

and

$$|\sum_{j=1}^{N}\psi(f(x_j))| \geq N(1-2\pi(\frac{1}{p}+\epsilon)) \tag{2.8}$$

Moreover considering F_q as an F_p vector space if $x_1,x_2,\ldots,x_N$ are colinear over F_p; i.e. there exists $w\in F_q$ such that $x_j=wc_j$, $c_j\in F_p$ $j=1,2,\ldots,N$; then n must satisfy

$$n+1 \geq \frac{N\log[\frac{p+p\epsilon}{1+p\epsilon}]}{\log p}+\frac{\log(1+[\frac{p+p\epsilon}{1+p\epsilon}]^{-N})}{\log p} \tag{2.9}$$

instead of inequality (2.7).

3.2 Notation and Lemmas

In the chapter $(\frac{\cdot}{q})$ will represent (generalized) Legendre symbol for F_q defined as follows :

$$(\frac{a}{q})=\begin{cases} 0 & \text{if } a=0 \\ 1 & \text{if } a\neq 0 \text{ and } a \text{ is a square in } F_q \\ -1 & \text{if } a \text{ is not a square in } F_q \end{cases}$$

We will prove three lemmas. Lemma 1 is used for Theorem 6.

Lemma 1 *Let $q=p^m$, p a prime number, $B=\{x_1,x_2,\ldots,x_N\}\subseteq F_q$ an arbitrary subset of F_q, and $1\leq n<N\leq q$. Moreover let A_n denote the set of polynomials in $F_q[x]$ having the properties:*

(i) the degrees of polynomials are $\leq n$,

(ii) the polynomials have no root in B,

(iii) the polynomials are not of the form $g(x)^2 h(x)$ *where* $g(x)$ *is a monic irreducible polynomial of degree* ≥ 1.

Then

$$|A_n| \geq q^{n+1}((1 - \frac{1}{q})^N - K_q) + C_{q,N,n} \tag{2.10}$$

where

$$0 \leq K_q \leq 5 \log \frac{q}{q-1} \tag{2.11}$$

and

$$|C_{q,N,n}| \leq \binom{N}{n+1} \tag{2.12}$$

PROOF. Let E_1 be the set of all polynomials in $F_q[x]$ whose degrees $\leq n$ and which have at least one root in B. Let E_2 be the set of all polynomials in $F_q[x]$ whose degrees $\leq n$ and which have no root in B. Then using exclusion-inclusion arguments we have

$$|E_2| = q^{n+1} - |E_1|$$

and

$$|E_1| = \binom{N}{1} q^n - \binom{N}{2} q^{n-1} + \ldots + (-1)^{n+1} \binom{N}{n} q$$

so

$$\begin{aligned} |E_2| &= q^{n+1}((1 - \frac{1}{q})^N - ((-1)^{n+1} \binom{N}{n+1} \frac{1}{q^{n+1}} + \ldots + (-1)^N \binom{N}{N} \frac{1}{q^N})) \\ &= q^{n+1}(1 - \frac{1}{q})^N + C_{q,N,n} \end{aligned}$$

where

$$|C_{q,N,n}| \leq \binom{N}{n+1}$$

Let S be the set of all polynomials of degree $\leq n$ and of the form $g(x)^2 h(x)$ where $g(x)$ is a monic irreducible polynomial of degree ≥ 1. Let S_k be the set of all polynomials in S of the form $g_k(x)^2 h(x)$ where g_k is a monic irreducible polynomial of degree k. Then

$$|S| \leq \sum_{k=1}^{[\frac{n}{2}]} |S_k|$$

It is well-known that (see for example [8] p. 93) the number of monic irreducible polynomials of degree k is

$$N_q(k) = \frac{1}{k} \sum_{d|k} \mu(d) q^{k/d} = \frac{1}{k} q^k c_k$$

where μ is Mobius function and

$$1 - \frac{q^k - q}{q^k(q-1)} \leq c_k \leq 1$$

Then using exclusion-inclusion arguments

$$|S_k| \leq \binom{q^k/k}{1} q^{n+1-2k} + \ldots + (-1)^{[\frac{n}{2k}]+1} \binom{q^k/k}{[\frac{n}{2k}]} q^{n+1-[\frac{n}{2k}]2k}$$

where we used generalized binomial coefficients.

$$|S_k| \leq q^{n+1}(\frac{1}{kq^k}) + q^{n+1} R'_k \text{ where } |R'_k| \leq \frac{1}{kq^{2k}}$$

$$\sum_{k=1}^{[\frac{n}{2}]} |S_k| \leq q^{n+1} \log \frac{q}{q-1} + q^{n+1} R' \text{ where } R' \leq 4 \log \frac{q^2}{q^2-1}$$

so

$$|S| \leq q^{n+1} 5 \log \frac{q}{q-1}$$

Therefore

$$|A_n| \geq |E_2| - |S| \geq q^{n+1}(1 - \frac{1}{q})^N + C_{q,N,n} - q^{n+1} 5 \log \frac{q}{q-1}$$

$$|A_n| \geq q^{n+1}((1 - \frac{1}{q})^N - K_q) + C_{q,N,n} \tag{2.13}$$

∎

The set A_n includes the set of all of the irreducible polynomials of degree n. Stepanov used this subset instead of A_n. Since A_n has more elements our bound is slightly better than Stepanov's bound.

Lemma 2 and Lemma 3 are used for Theorem 7'. Lemma 2 is a special case of Lemma 3 with a better bound.

Lemma 2 *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ be given and $1 \leq n < N \leq q$. Moreover let $x_1, x_2, \ldots, x_N$ be colinear over F_p. Define A_n as the set of all polynomials in $F_q[x]$ of degree $\leq n$. Let τ be the linear map between the F_p vector spaces*

$$\tau : A_n \to \prod_{i=1}^{N} F_p \tag{2.14}$$

with

$$\tau(f) = (tr(f(x_1)), tr(f(x_2)), \ldots, tr(f(x_N))) \tag{2.15}$$

Then the rank of the corresponding matrix is $\geq n + 1$.

PROOF. Each $f \in A_n$ can be written as $f(x) = \sum_{k=0}^{n} a_k x^k$, $a_k \in F_q$. There exits a normal basis $\{w_1, w_2, \ldots, w_m\} \subseteq F_q$ for F_q as a vector space over F_p such that $w_i = w^{p^{i-1}}, i = 1, 2, \ldots, m$ for some $w \in F_q$. Then

$$a_k = \textstyle\sum_{j=1}^{m} \alpha_{k,j} w_j, \quad \alpha_{k,j} \in F_p,$$

$$f(x) = \sum_{k=0}^{n} \sum_{j=1}^{m} \alpha_{k,j} w_j x^k$$

By additivity of trace

$$tr(f(x)) = \sum_{k=0}^{n} \sum_{j=1}^{m} \alpha_{k,j} tr(w_j x^k)$$

Thus the matrix of this map is

$$A_{N,B} = \begin{bmatrix} tr(w_1) & tr(w_m) & tr(w_1 x_1) & tr(w_m x_1) & tr(w_1 x_1^n) & tr(w_m x_1^n) \\ tr(w_1) & tr(w_m) & tr(w_1 x_2) & tr(w_m x_2) & tr(w_1 x_2^n) & tr(w_m x_2^n) \\ \vdots & \vdots & \vdots & & \vdots & \\ tr(w_1) & tr(w_m) & tr(w_1 x_N) & tr(w_m x_N) & tr(w_1 x_N^n) & tr(w_m x_N^n) \end{bmatrix}$$

$$\begin{bmatrix} tr(w_1) & tr(w_j x_1) \\ tr(w_1) & tr(w_j x_2) \end{bmatrix} \text{ is a submatrix of } A_{N,B}$$

$tr(w_j) \neq 0$ for any $j = 1, 2, \ldots, m$. Moreover for some j, $1 \leq j \leq m$ $tr(w_j(x_2 - x_1)) \neq 0$, if $x_2 \neq x_1$; since otherwise $tr(\alpha(x_2 - x_1)) = 0$ for each $\alpha \in F_q$ so $tr(\beta) = 0$ for each $\beta \in F_q$. Then rank $A_{N,B} \geq 2$. Define

$A_{N,B}(j_1, j_2, \ldots, j_n)$, $1 \leq j_i \leq m$, $i = 1, 2, \ldots, n$,which is a submatrix of $A_{N,B}$, as below

$$A_{N,B}(j_1, j_2, \ldots, j_n) = \begin{bmatrix} tr(w_1) & tr(w_{j_1} x_1) & tr(w_{j_2} x_1^2) & tr(w_{j_n} x_1^n) \\ tr(w_1) & tr(w_{j_1} x_2) & tr(w_{j_2} x_2^2) & tr(w_{j_n} x_2^n) \\ & & & \\ & & & \\ tr(w_1) & tr(w_{j_1} x_{n+1}) & tr(w_{j_2} x_{n+1}^2) & tr(w_{j_n} x_{n+1}^n) \end{bmatrix}$$

Using the facts that

(i) $x_1, x_2, \ldots, x_N$ are colinear over F_p,

(ii) $A_{N,B}(j_1, j_2, \ldots, j_n)$ is similar to Vandermonde matrix,

we can bring $A_{N,B}(j_1, j_2, \ldots, j_n)$ into an equivalent form $\bar{A}_{(j_1,j_2,\ldots,j_n),N,B}$ which is

$$A_{N,B}(j_1, j_2, \ldots, j_n) = \begin{bmatrix} tr(w_1) & * & * \\ 0 & tr(w_{j_1}(x_2 - x_1)) & * \\ & & \\ & & \\ 0 & 0 & tr(w_{j_n}(x_n - x_{n-1})(x_{n-1} - x_{n-2}) \cdots (x_2 - x_1)) \end{bmatrix}$$

where $*$ represents a don't-care entry. Since $x_{j_1} \neq x_{j_2}$ if $j_1 \neq j_2$, $\bar{A}_{N,B}(j_1, j_2, \ldots, j_n)$ is nonsingular. Therefore rank $\tau \geq n + 1$. ∎

Lemma 3 *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ be given and*
$1 \leq n < N \leq q$. Define A_n as the set of all polynomials in $F_q[x]$ of degree $\leq n$. Let τ be the linear map between the F_p vector spaces

$$\tau : A_n \rightarrow \prod_{i=1}^{N} F_p \tag{2.16}$$

with

$$\tau(f) = (tr(f(x_1)), tr(f(x_2)), \ldots, tr(f(x_N))) \tag{2.17}$$

Then the rank of the corresponding matrix is $\geq [\frac{n+1}{m}]$.

PROOF. We know $f(x) = \sum_{k=0}^{n}\sum_{j=1}^{m} \alpha_{k,j} w_j x^k$ where $\alpha_{k,j} \in F_p$, $w_j = w^{p^{j-1}}$ forming a normal basis.

$$tr(f(x)) = f(x)+f(x)^p+\cdots+f(x)^{p^{m-1}} \text{ and } (f(x))^{p^\nu} = \sum_{k=0}^{n}\sum_{j=1}^{m} \alpha_{k,j} w_j^{p^\nu} x^{kp^\nu},\ 0 \le \nu \le m-1$$

Define $\xi_{i,\nu} = x_i^{p^\nu}, i = 1, 2, \cdots, N$. By normality of the basis $w_j^{p^\nu} = w_{j+\nu}$. Therefore $f \in Ker(\tau)$ if and only if

$$tr(f(x_i)) = \sum_{\nu=0}^{m-1}\sum_{k=0}^{n}\sum_{j=1}^{m} \alpha_{k,j} w_{j+\nu} \xi_{i,\nu}^k = 0 \text{ for each } 1 \le i \le N \qquad (2.18)$$

We can write the system (2.18) in matrix notation as follows

$$(\tilde{A}_{N,B})_{N\times(n+1)m^2}(\tilde{b}_{N,B})_{(n+1)m^2\times 1} = (0)_{N\times 1} \qquad (2.19)$$

where

$$\tilde{A}_{N,B} = \begin{bmatrix} A_{1,0} & A_{1,1} & & A_{1,m-1} \\ A_{2,0} & A_{2,1} & & A_{2,m-1} \\ & & & \\ A_{N,0} & A_{N,1} & & A_{N,m-1} \end{bmatrix},\ \tilde{b}_{N,B} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{bmatrix}$$

with

$$A_{i,\nu} = \begin{bmatrix} \overbrace{1\ldots 1}^{m\ times} & \overbrace{\xi_{i,\nu}\ldots\xi_{i,\nu}}^{m\ times} & & \overbrace{\xi_{i,\nu}^n\ldots\xi_{i,\nu}^n}^{m\ times} \end{bmatrix},\ b_\nu = \begin{bmatrix} \alpha_{0,1}w_{1+\nu} \\ \alpha_{0,2}w_{2+\nu} \\ \\ \alpha_{0,m}w_{m+\nu} \\ \alpha_{1,1}w_{1+\nu} \\ \alpha_{1,2}w_{2+\nu} \\ \vdots \\ \alpha_{1,m}w_{m+\nu} \\ \\ \vdots \\ \alpha_{n,1}w_{1+\nu} \\ \alpha_{n,2}w_{2+\nu} \\ \\ \alpha_{n,m}w_{m+\nu} \end{bmatrix}$$

There is a natural isomorphism between F_p vector spaces A_n and $\prod_{i=1}^{(n+1)m} F_p$. Therefore $Ker(\tau) = \{(\alpha_{0,1}, \ldots, \alpha_{0,m}, \alpha_{1,1}, \ldots, \alpha_{1,m}, \ldots, \ldots, \alpha_{n,1}, \ldots, \alpha_{n,m}) \in \prod_{i=1}^{(n+1)m} F_p : \tilde{b}_{N,B}$ formed with this vector satisfies (2.18)$\}$.

But we can observe that in $\tilde{b}_{N,B}$ for each $\alpha_{k,j}$ there exists m enteries as $\alpha_{k,j}w_l$, $1 \leq l \leq m$. For $v = 0$ we have a submatrix $A^*_{N,B}$ of $\tilde{A}_{N,B}$

$$A^*_{N,B} = \begin{bmatrix} 1 & \xi_{1,0} & \xi^n_{1,0} \\ 1 & \xi_{2,0} & \xi^n_{2,0} \\ \vdots & \vdots & \vdots \\ 1 & \xi_{n+1,0} & \xi^n_{n+1,0} \end{bmatrix} = \begin{bmatrix} 1 & x_1 & x_1^n \\ 1 & x_2 & x_2^n \\ \vdots & \vdots & \vdots \\ 1 & x_{n+1} & x^n_{n+1} \end{bmatrix}$$

which is a Vandermonde matrix.

Therefore $dim\{\tilde{b}_{N,B} \in \prod_{i=1}^{(n+1)m^2} F_p : \tilde{b}_{N,B}$ satisfying (2.18)$\} \leq (n+1)m^2 - (n+1)$. Since there is an m to 1 map from this kernel $\in \prod_{i=1}^{(n+1)m^2} F_p$ to $Ker(\tau) \in \prod_{i=1}^{(n+1)m} F_p$, we have $dim(Ker(\tau)) \leq -[-(n+1)m + \frac{n+1}{m}]$. Therefore

$$rank(\tau) \geq (n+1)m + [-(n+1)m + \frac{n+1}{m}] = [\frac{n+1}{m}]$$

∎

3.3 Proof of Theorem 6

First we will prove Theorem 6 for generalized Legendre symbol in Proposition 1.

Proposition 1 *Let $q = p^m$, p an odd prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ an arbitrary subset of F_q. Assume $N = c(q)\log q$ and $n \geq 1$ is an integer satisfying*

$$n \geq \frac{\mathrm{N}\log 2}{\log q} - \frac{\mathrm{N}\log(1-\frac{1}{q}) + \log(1 - \mathrm{K_q}(1-\frac{1}{q})^{-\mathrm{N}})}{\log q} + \frac{\log(1-2^{-\mathrm{N}})}{\log q} + \mathrm{R_{N,q}} \quad (2.20)$$

where

$$0 \leq K_q \leq 5\log\frac{q}{q-1} \quad (2.21)$$

and

$$|R_{N,q}| \leq (M\frac{\log q}{q})^2 \frac{1}{(1-\frac{1}{q})^N - K_q} \quad (2.22)$$

and also where

(i) if $c(q) \to \infty$ *as* $q \to \infty$, *then* $M = \frac{c}{\log 2}$

(ii) if there exits C' *such that* $c(q) \leq C'$ *as* $q \to \infty$, *then* $M = C'$

Then there exists a monic square free polynomial $f(x)$ *in* $F_q[x]$ *of degree* $\leq 2n$ *such that*

$$\sum_{j=1}^{N}(\frac{f(x_j)}{q}) = N$$

where $(\frac{\cdot}{q})$ *is the generalized Legendre symbol.*

PROOF. Let A_n^* be the set of all monic polynomials in A_n, which is the set defined in Lemma 1. Then

$$|A_n^*| = \frac{|A_n|}{q} \geq q^n((1-\frac{1}{q})^N - K_q) + \frac{C_{q,N,n}}{q}$$

For each polynomial in A_n^* assign an N*–tuple* as follows

$$f_i \in A_n^* \longmapsto \gamma_i \in \prod_{i=1}^{N}\{-1,1\}$$

$$\gamma_i = ((\frac{f_i(x_1)}{q}),(\frac{f_i(x_2)}{q}),\ldots,(\frac{f_i(x_N)}{q}))$$

If $|A_n^*| \geq 2^N + 1$, then there exits at least two equal N*–tuples* $\gamma_1 = \gamma_2$ where $f_1 \not\equiv f_2$. Define f as $f = f_1 f_2$.Since f_i is a square-free polynomial $i = 1, 2$, f is not a square polynomial. Moreover $(\frac{f(x_j)}{q}) = 1$ for each $j = 1, 2, \ldots, N$.So

$$\sum_{j=1}^{N}(\frac{f(x_j)}{q}) = N \text{ and } degf \leq 2n$$

and

$$2^N + 1 \leq q^n((1-\tfrac{1}{q})^N - K_q) + \tfrac{C_{q,N,n}}{q} \leq |A_n^*| \text{ whenever}$$

$$n \geq \frac{N\log 2}{\log q} - \frac{N\log(1-\frac{1}{q}) + \log(1 - K_q(1-\frac{1}{q})^{-N})}{\log q} + \frac{\log(1+2^{-N})}{\log q} + \log(1 + \frac{C_{q,N,n}}{q^{n+1}((1-\frac{1}{q})^N - K_q)})$$

If $c(q) \leq C'$, then $\binom{N}{n+1} \leq \frac{N^{n+1}}{(n+1)!} \leq (C'\log q)^{n+1}$.

If $c(q) \to \infty$ as $q \to \infty$, then $n+1 \to \infty$ as $q \to \infty$ and using Stepanov's result

$$n \geq \frac{(N+1)\log 2}{\log q} + 1 \Longrightarrow \frac{N}{n+1} \leq \frac{\log q}{\log 2}$$

Now using Stirling's formula for $\binom{N}{n+1}$, i.e.

$$\log N! = (N+\tfrac{1}{2})\log N - N + C + O(\tfrac{1}{N}) \text{ where } C = \tfrac{1}{2}\log 2\pi \text{ as } q \to \infty$$

we get

$$\binom{N}{n+1} = (\frac{N}{n+1})^{n+1}\frac{1}{\sqrt{n+1}}e^{(n+1)(1-\frac{2n+1}{2N})(1-O(\frac{n+1}{N}))-C+O(\frac{1}{n+1}+\frac{1}{N-n-1})}$$

So

$$\binom{N}{n+1} \le (\frac{\log q}{\log 2})^{n+1}e^{n+1} = (\frac{e}{\log 2}\log q)^{n+1}$$

Thus $|C_{q,N,n}| \le (M\log q)^{n+1}$ where if $c(q)$ is bounded by C' ,then $M \ge C'$; else $M = \frac{e}{\log 2}$. But

$$|\log(1+\frac{C_{q,N,n}}{q^{n+1}((1-\frac{1}{q})^N - K_q)})| \le (M\frac{\log q}{q})^2\frac{1}{(1-\frac{1}{q})^N - K_q}$$

Thus

$$n \ge \frac{N\log 2}{\log q} - \frac{N\log(1-\frac{1}{q}) + \log(1-K_q(1-\frac{1}{q})^{-N})}{\log q} + \frac{\log(1-2^{-N})}{\log q} + R_{N,q}$$

where $|R_{N,q}| \le (M\frac{\log q}{q})^2\frac{1}{(1-\frac{1}{q})^N - K_q}$

If $f(x)$ is square free , then we are done. Otherwise $f(x) = f'(x)(g(x))^2$ where $f'(x)$ is a square free polynomial. Thus $deg f'(x) \le deg f(x)$ and $(\frac{f'(x)}{q}) = (\frac{f(x)}{q})$ for each $x \in B$. Therefore $f'(x)$ satisfies the conditions. ∎

This proposition easily extends to the case of general multiplicative characters.

PROOF. [Proof of Theorem 6] Assume f_1 and f_2 are distinct polynomials of degree $\le n$, not vanishing in B and they are not of the form $g(x)^2h(x)$, where $g(x)$ is a monic irreducible polynomial, i.e. square-free. Then

$$f_1^{i_1}f_2^{s-i_1} \equiv f_1^{i_2}f_2^{s-i_2} \Leftrightarrow f_1^{i_1-i_2} \equiv f_2^{i_1-i_2} \Leftrightarrow i_1 = i_2$$

by unique factorization. Let A_n^* be the set defined in the proof of Proposition 1. We know

$$|A_n^*| = \frac{|A_n|}{q} \ge q^n((1-\frac{1}{q})^N - K_q) + \frac{C_{q,N,n}}{q}$$

$$\text{where } 0 \le K_q \le 5\log\frac{q}{q-1} \text{ and } |C_{q,N,n}| \le \binom{N}{n+1}$$

Thus if

$$q^n((1-\frac{1}{q})^N - K_q) + \frac{C'_{q,N,n}}{q} \geq s^N + 1 \tag{2.23}$$

there exist at least two polynomials $f_1 \not\equiv f_2$ such that

$$\chi(f_1(x_j)) = \chi(f_2(x_j)) \text{ for each } j = 1, 2, \ldots, N$$

Define $h_i = f_1^i f_2^{s-i}$, $i = 1, 2, \ldots, s-1$. Then

$$\chi(h_i(x_j)) = \chi(f_1^i(x_j))\chi(f_2^{s-i}(x_j)) = \chi(f_2^s(x_j)) = 1 \text{ for each } j = 1, 2, \ldots, N$$

Moreover $h_{i_1} \not\equiv h_{i_2}$ if $i_1 \neq i_2$, $i_l = 1, 2, \ldots, s-1$. Therefore if the inequality (2.23) is satisfied, then there exists (s-1) distinct monic polynomials satisfying the condition which are not in $(P_q[x])^s$. The inequality is satisfied whenever

$$n \geq \frac{N \log s}{\log q} - \frac{N \log(1-\frac{1}{q}) + \log(1 - K_q(1-\frac{1}{q})^{-N})}{\log q} + \frac{\log(1+s^{-N})}{\log q} + \log(1 + \frac{C_{q,N,n}}{q^{n+1}((1-\frac{1}{q})^N - K_q)})$$

If $c(q) \leq C'$,then $\binom{N}{n+1} \leq \frac{N^{n+1}}{(n+1)!} \leq (C' \log q)^{n+1}$.

If $c(q) \to \infty$ as $q \to \infty$, then we can extend Stepanov's result for any multiplicative character of exponent s such that

if $s^N + 1 \leq \frac{q^n}{2n}$ there are $s-1$ different nontrivial polynomials which are mapped to 1 at each point in B. This implies

$$\frac{N}{n+1} \leq \frac{N \log q}{N \log s + \log(1+s^{-N}) + \log(2n) + \log s} \leq \frac{\log q}{\log s}$$

By using Stirling's formula $\binom{N}{n+1} \leq (\frac{\log q}{\log s})^{n+1} e^{n+1} = (\frac{e}{\log s} \log q)^{n+1}$. So we can take $M = \frac{e}{\log s}$. Thus

$$|\log(1 + \frac{C'_{q,N,n}}{q^{n+1}((1-\frac{1}{q})^N - K_q)})| \leq (M \frac{\log q}{q})^2 \frac{1}{(1-\frac{1}{q})^N - K_q}$$

Similar to the proof of Proposition 1, if $h_i(x)$ is not s power free, then $h_i(x) = h'_i(x)(g_i(x))^s$ where $h'_i(x)$ is s power free and satisfies the conditions for $i = 1, 2 \ldots (s-1)$. ∎

3.4 Proof of Theorem 7 and Theorem 7′

PROOF. [Proof of Theorem 7]

Let $1 \leq n \leq q^{1/2}$ be an integer. Define $k = [\frac{n}{p}]$. Let C be the set of all polynomials f in $F_q[x]$ which are not identically zero having the property that $1 \leq deg f \leq n$ and the coefficients of x^{pi} are zero for each $i = 0, 1, \ldots, k$. Namely
$C = \{(a_1 x + \cdots + a_{p-1}x^{p-1}) + (a_{p+1}x^{p+1} + \cdots + a_{2p-1}x^{2p-1}) + \cdots + (a_{kp+1}x^{kp+1} + \cdots + a_n x^n) \mid a_i \in F_q$, not each a_i is zero $\}$
Then the cardinality of C is $|C| = q^{n-[\frac{n}{p}]} - 1$. If $f_1, f_2 \in C$ and $f_1 \neq f_2$, then $(deg(f_1 - f_2), p) = 1$. So since $deg(f_1 - f_2) \leq n \leq q^{1/2}$ by Weil's theorem for additive characters (see for example [8] theorem 5.28 page 223) $tr(f_1 - f_2)(F_q) \neq \{0\}$.

Let $K = [\frac{p-1}{p\epsilon} + 1]$. Define $U_i = [(i-1)\epsilon, i\epsilon)$, $1 \leq i \leq K$ as an interval in $[0, \frac{p-1}{p} + \epsilon)$ and $\frac{p-1}{p} \in U_K$. $U_i \cap U_j = \emptyset$ if $i \neq j$. For each $f \in C$ define an N-tuple as follows:

$$\Gamma(f) = (l_1, l_2, \ldots, l_N) \text{ where } \frac{tr(f(x_i))}{p} \in U_{l_i},\ l_i \in 1, 2, \ldots, K \text{ and } 1 \leq i \leq N.$$

There are K^N distinct values on the image of Γ. If $|C| \geq K^N + 1$ there are at least two distinct polynomials f_1, f_2 in C such that

$$|\frac{tr(f_1 - f_2)(x_i)}{p}| \leq \epsilon \text{ for each } i = 1, 2, \ldots, N$$

Let $f = f_1 - f_2$. Then

$$|\sum_{i=1}^{N} \psi(f(x_i))| = |\sum_{i=1}^{N} e^{2\pi i \frac{tr(f(x_i))}{p}}| \geq \sum_{i=1}^{N} Re(e^{2\pi i \frac{tr(f(x_i))}{p}}) = \sum_{i=1}^{N} \cos(2\pi \frac{tr(f(x_i))}{p})$$

Using $\cos x = \cos |x| \geq 1 - |x|$

$$\cos(2\pi \frac{tr(f(x_i))}{p}) \geq 1 - 2\pi\epsilon. \text{ Thus } |\sum_{i=1}^{N} \psi(f(x_i))| \geq N(1 - 2\pi\epsilon)$$

We know $|C| = q^{n-[\frac{n}{p}]} - 1$. Thus whenever $K^N + 1 \leq q^{n-[\frac{n}{p}]} - 1$ the existence of such f is guaranteed. But this means

$$n - [\frac{n}{p}] \geq \frac{N \log([\frac{p-1}{p\epsilon} + 1]) + \log(2 + [\frac{p-1}{p\epsilon} + 1]^{-N})}{m \log p}$$

∎

PROOF. [Proof of Theorem 7'] Let A_n be the set of all polynomials in $F_q[x]$ whose degree $\leq n$. Let $f_1 \in A_n$. Denote by k the $dim(Ker(\tau))$ and let $r = rank(\tau)$ where τ is the map defined in lemmas. Then define

$$S_1 = \{g_1 \in A_n : tr((g_1 - f_1)(x_i)) = 0 \text{ for each } i = 1, 2, \ldots N\} \subseteq A_n$$

Let $f_2 \in A_n \setminus S_1$. Define

$$S_2 = \{g_2 \in A_n : tr((g_2 - f_2)(x_i) = 0 \text{ for each } i = 1, 2, \ldots N\} \subseteq A_n$$

Let $f_j \in A_n \setminus \bigcup_{i=1}^{j-1} S_i$ for $j = 3, 4, \ldots, m$ where

$$S_j = \{g_j \in A_n : tr((g_j - f_j)(x_i) = 0 \text{ for each } i = 1, 2, \ldots N\} \subseteq A_n$$

Thus $|S_j| = p^k$ for $j = 1, 2, \ldots, l$ and $l = p^r$. Define $C = \{f_1, f_2, \ldots, f_l\} \subseteq A_n$. $|C| = p^r$ and $r \geq [\frac{n+1}{m}]$ (respectively $n+1$ if $\{x_1, x_2, \ldots, x_N\}$ are colinear) by Lemma 3 (resp. Lemma 2).

Let $K = [\frac{p+p\epsilon}{1+p\epsilon}]$. Define $U_i = [(i-1)(\frac{1}{p}+\epsilon), i(\frac{1}{p}+\epsilon))$, $1 \leq i \leq K$ as an interval in $[0, 1+\epsilon)$ and $\frac{p-1}{p} \in U_K$. By similar arguments as in the proof of Theorem 7, if $K^N + 1 \leq p^r \leq p^{[\frac{n+1}{m}]}$ (resp. p^{n+1}) there exists a polynomial f of degree $\leq n$ such that

$$|\sum_{i=1}^{N} \psi(f(x_i))| \geq N(1 - 2\pi(\frac{1}{p} + \epsilon))$$

But this means

$$[\frac{n+1}{m}] \text{ (resp. } n+1) \geq \frac{N \log[\frac{p+p\epsilon}{1+p\epsilon}] + \log(1 + [\frac{p+p\epsilon}{1+p\epsilon}]^{-N})}{\log p}$$

Moreover $tr(f(B)) \neq \{0\}$ by Lemma 3 (resp. Lemma 2). ∎

Chapter 4

PRELIMINARIES 2

This chapter contains just definitions of linear codes and geometric Goppa codes. For detailed exposition see Stepanov [2], Stichtenoth [9], or van Lint [17].

4.1 Linear Codes

Let F_q be a finite field with q elements, and $F_q^n = F_q \times \cdots \times F_q$ n-dimensional vector space over F_q. We can define a metric d on F_q^n as

$$d(x, y) = \sum_{\substack{i=1 \\ x_i \neq y_i}}^{n} 1,$$

where $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in F_q^n$.

A *linear code* $[n, k, d]_q$ is a k-dimensional subspace of the vector space F_q^n, where d is the minimum distance between codewords, i.e. elements of the code.

The relative parameters of of the linear code $[n, k, d]_q$ are defined as

1. $R = \dfrac{k}{n}$, called as *rate*,
2. $\delta = \dfrac{d}{n}$, called as *relative minimum distance*.

There exists a bound on d

$$d \leq n - k + 1$$

which is called as the *Singleton Bound*. In relative parameters this means

$$R \leq 1 - \delta + \frac{1}{n}.$$

The codes achiving this bound are called as *maximal codes*.

By a "good" code $[n, k, d]_q$ we mean

1. n is large, for instance compared to q,
2. the Singleton Bound is nearly achieved.

4.2 Geometric Goppa Codes

Let $k = F_q$, a finite field with q elements, X a smooth projective curve over $\bar{F}_q$, the algebraic closure of F_q. Let $D_0 = P_1 + \cdots + P_n$ be a divisor of degree n where $P_i \neq P_j$ if $i \neq j$. Let D be another divisor whose support is disjoint from the support of D_0. Let $L(D) = \{f \in k(X)^* : (f) + D \geq 0\} \cup \{0\}$ be the linear space of rational functions on X over k. Then the corresponding *geometric Goppa code* $C(D_0, D)$ is the image of the linear map

$$Ev : L(D) \to F_q^n,$$
$$f \mapsto (f(P_1), \ldots, f(P_n)).$$

Chapter 5

CODES ON SUPERELLIPTIC CURVES

5.1 Introduction

In chapter 3 we extended Stepanov's approach, which gives a constructable proof of the fact that Weil's estimate (see section 2.4) is attainable for any F_q.

In this chapter we apply Goppa's construction (see for example [2]) to the curve over F_q

$$y^s = f(x)$$

where f is obtained by Stepanov's approach to attain

$$\sum_{x \in F_q} \chi(f(x)) = q$$

where χ is a multiplicative character of exponent s and $s \mid q-1$.

Theorem 8 *Let F_q be a finite field of characteristic p, s an integer $s \geq 2$, $s \mid (q-1)$, and c be the infimum of the set*

$$C = \{x : \text{a non-negative real number} \mid \text{there exists an integer } n \text{ such that } \frac{q^x(q-2)}{(q-1)(s-1)(1+\frac{1}{s^q(s-1)})} \geq n \geq \frac{q \log s}{\log q} + x\}.$$

Let r be an integer satisfying

$$s(s-1)\lceil \frac{q \log s}{\log q} + c \rceil - 2s < r < sq.$$

Then there exists a linear code $[n, k, d]_q$ *with parameters*

$$\begin{aligned} n &= sq, \\ k &= r - \tfrac{s(s-1)}{2}\lceil \tfrac{q \log s}{\log q} + c \rceil + s, \\ d &\geq sq - r. \end{aligned}$$

Corollary 2 *Under the same conditions with Theorem 8, there exists a code with relative parameters satisfying*

$$R \geq 1 - \delta - \frac{\frac{s(s-1)}{2}\lceil \frac{q \log s}{\log q} + c \rceil - s}{sq}.$$

Remark 2 *When* $s << q$*, we have for Corollary 2*

$$R \geq 1 - \delta - J_1(s, q)$$

where $J_1(s, q) \sim \frac{(s-1)\log s}{2} \frac{1}{\log q}$*. Although* $\frac{1}{q^{\frac{1}{2}}} << \frac{1}{\log q}$*, Theorem 8 is significant espccially when* q *is a prime.*

5.2 Proof of Theorem 8

PROOF. Let χ be a multiplicative character of exponent s of F_q. If $m \geq \frac{q \log s}{\log q} + c$, then $\frac{1}{m} q^m \frac{q-2}{q-1} \geq (s-1)s^q + 1$. Note that the number of monic irredicible polynomials of degree m over F_q is $\frac{1}{m}\sum_{d|m} \mu(d) q^{m/d} = \frac{1}{m} q^m c_m$ (see for example [8] page 93). Here $1 \geq c_m \geq 1 - \frac{q^m - q}{q^m(q-1)} \geq \frac{q-2}{q-1}$. Forming q-tuples for each irreducible monic polynomial as in the proof of Theorem 6; by Dirichlet's pigeon-hole principle if $\frac{1}{m} q^m \frac{q-2}{q-1} \geq (s-1)s^q + 1$, there exists a square-free polynomial $f \in F_q[x]$ of degree $\leq ms$ such that $\chi(f(a)) = 1$ for each $a \in F_q$. Let $\deg f = s\lceil \frac{q \log s}{\log q} + c \rceil$.

Since $s \mid (q-1)$ there are s many multiplicative characters of exponent s over F_q. Moreover for any χ of exponent s, $\chi(f(a)) = 1$ for all $a \in F_q$. Therefore we have over the curve

$$y^s = f(x)$$

$n = N_q = sq$ many F_q-rational points (see Schmidt [7] page 79 or Stepanov [1], p.51).

Using the well-known genus formulas for superelliptic curves (see for example Stichtenoth [9] p. 196), the geometric genus is given by

$$g = \frac{s(s-1)}{2}\lceil \frac{q \log s}{\log q} + c \rceil - s + 1.$$

Let D_0 be the divisor on the smooth model X of $y^s = f(x)$ where

$$D_0 = \sum_1^n x_i$$

By tracing the normalization of a curve one sees that the number of rational points of a non-singular model $\bar{C}$ of a curve C is more than the number of rational points of C (see for example Shafarevich [10], section 5.3). Thus $n = \deg D_0 \geq N_q = sq$. Let x_∞ be a point of X at infinity, $D = rP_\infty$ be the divisor of degree r and $supp\ D_0 \cap supp\ D = \emptyset$, where r to be determined. If

$$2g - 2 < r < N_q,$$

by using the Goppa construction,

$$n = N_q, \quad k = r + 1 - g, \quad d \geq N_q - r.$$

∎

Chapter 6

CONCLUSION

Theorem 6 is an extension of S.A. Stepanov's result [3] and the bound we have found is slightly better. Theorem 8 uses the same ideas for construction of superelliptic curves with a lot of rational points. It is especially important when F_q is a prime finite field since most of the known "good" codes at present are constructed over extension fields.

It is possible to apply Gluhov's polynomials [5] , [6] as in Theorem 8, so that we can get fairly good codes even for odd extensions of finite fields. See [18] .

There is a new method giving even longer codes with "good" parameters, which has been proved by S.A. Stepanov [19] recently, using complete intersections.

REFERENCES

[1] S.A. Stepanov, "Arithmetic of Algebraic Curves", Plenum, New York, 1994.

[2] S.A. Stepanov, "Error-Correcting Codes and Algebraic Curves", to be published.

[3] S.A. Stepanov, "On lower estimates of incomplete character sums of polynomials", Proceedings of the Steklov Institue of Mathematics, AMS, 1980 Issue 1, 187-189.

[4] S.A. Stepanov, "On lower bounds of sums of characters over finite fileds", Discrete Math. Appl., 1992, Vol. 2, no. 5, 523-532.

[5] M.M. Gluhov, "Lower bounds for character sums over finite fields", Diskrt. Math., 1994, 6, no. 3, 136-142 (in Russian).

[6] M.M. Gluhov, "On lower bounds for character sums over finite fileds", preprint, 1995.

[7] Wolfgang M. Schmidt, "Equations over Finite Fields An Elementary Approach", Lecture Notes in Mathematics 536, Springer-Verlag, 1976.

[8] Rudolf Lidl and Harald Niederreiter, "Finite Fields", Encylopedia of Mathematics and It's Applications vol 20, Cambridge University Press, 1984.

[9] H. Stichtenoth, "Algebraic Function Fields and Codes", Springer-Verlag, 1993.

[10] I. R. Shafarevich, "Basic Algebraic Geometry 1", second edition, Springer-Verlag, 19994.

[11] A.Weil, "Numbers of solutions of equations in finite fileds", Bull. of the American Math. Soc., 55(1949), 497-508.

[12] A.A. Karatsuba, "Lower bounds for character sums of polynomials", Mat. Zametki 14(1973), 67-72; English trans. in Math Notes 14(1973).

[13] Karl K. Norton, "Bounds for sequences of consecutive power residues I", AMS Volume 24 Proceedings of Sym. in Pure Math., 1973, 213-220.

[14] P.D.T.A. Elliot, "Some notes on k-th power residues", Acta Arithm. 14(1967/68), 153-162.

[15] D.A. Mit'kin, "Lower bounds for sums of Legendre Symbols and trigonometric sums", Uspehi Mat. Nauk 30(1975).

[16] I. Niven, H.S. Zuckerman, H.L. Montgomery, "An Introduction to the Theory of Numbers", John Wiley & Sons, Inc., 1991.

[17] J.H. van Lint, "Introduction to Coding Theory", Graduate Texts in Mathematics 86, Springer Verlag, 1982.

[18] M.M. Gluhov-J.R. and F. Özbudak, "Codes on Superelliptic Curves", preprint, 1995.

[19] S.A. Stepanov, "Codes on Complete Intersections", preprint, 1995.